IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Brookner, George Application No.: 10/071,820 Filed: 02/07/2002 Title: Secure Data Capture Apparatus and Method Attorney Docket No.: ASCO.P-071	Group Art Unit: 3621 Examiner: Christina O. Sherr Confirmation No: 3786

BRIEF FOR APPELLANT

This brief is filed in support of Applicants' Appeal from the rejection mailed 12/02/2005. Consideration of the application and reversal of the rejections are respectfully urged.

(i) Real Party in Interest

The real party in interest is one or more of the following entities: assignee Ascom Hasler Mailing Systems, Inc., Hasler Mailing Systems Inc., Neopost Group, and Mailroom Technology Inc.

(ii) Related Appeals and Interferences

None

(iii) Status of Claims

The application was originally filed with 24 claims, and 24 claims are now pending. Claims 1-24 have all been rejected.

The rejection of claims 1-24 is appealed.

(iv) Status of Amendments

No amendment has been filed subsequent to the non-final rejection of December 2, 2005.

(v) Summary of Claimed Subject Matter

It is noted that the application was filed electronically and thus does not have unambiguous page and line numbers. For that reason, the numbered paragraphs of the electronically filed application are cited.

A summary of a first embodiment of the invention, typified by independent claim 1, follows.

In this embodiment, there is postage meter system, under the jurisdiction of a postal authority, comprising a host and a server. The host comprises a postal security device and postal indicia printing means. The server comprises a cryptographic device for making cryptographically secure communications with the postal security device. (See paragraphs 11 and 20; Figure 1)

Information about a batch of mail pieces about to franked is entered into the host. The mail pieces are franked while information about the franking of the mail pieces is stored to memory within the host. (See paragraphs 11, 19, 62, 63; Figure 1 and Figure 2)

A cryptographic authenticating procedure is performed upon both the information about the franking of the batch of mail pieces and the information about the batch of mail pieces. Both types of information are statistical information. (See paragraphs 11 and 64; Figure 2)

The statistical information is communicated from the postal storage device to the cryptographic

device where the statistical information is authenticated. The statistical information is then passed to a postal authority. (See paragraphs 11, 29, 64, 65, and 67; Figure 1 and Figure 2)

A summary of a second embodiment of the invention, typified by dependent claim 11 follows.

This embodiment is the same as the method of claim 1, with the exception of the following details.

The step where statistical information is communicated from the postal security device to the cryptographic device further comprises the following:

The statistical information within the postal security device is cryptographically signed, yielding a signature. (See paragraph 30)

The information and signature is communicated to memory within the host and not within the postal storage device. (See paragraph 32)

The information and signature is communicated from the memory within the host and not within the postal security device to the cryptographic device. (See paragraph 32)

A summary of a third embodiment of the invention, typified by claim 13 follows.

In this embodiment, there is postage meter system, under the jurisdiction of a postal authority, comprising a host and a server. The host comprises a postal security device and postal indicia printing means. The server comprises a cryptographic device for making cryptographically secure communications with the postal security device. (See paragraphs 11 and 20; Figure 1) In

this embodiment, the host is operated by a service provider which provides service to a plurality of users. (See paragraph 27 and Figure 1)

Information about a batch of mail pieces about to franked is entered into the host. This information is also indicative of the identity of a user associated with the batch. (See paragraph 48)

The mail pieces are franked while information about the franking of the mail pieces is stored to memory within the host. (See paragraphs 11, 19, 62, 63; Figure 1 and Figure 2)

A cryptographic authenticating procedure is performed upon both the information about the franking of the batch of mail pieces and the information about the batch of mail pieces. Both types of information are statistical information. (See paragraphs 11 and 64; Figure 2)

The statistical information is communicated from the postal storage device to the cryptographic device where the statistical information is authenticated. The statistical information is then passed to a postal authority. (See paragraphs 11, 29, 64, 65, and 67; Figure 1 and Figure 2)

A summary of a fourth embodiment of the invention, typified by claim 23, as follows.
This embodiment is the same as the method of claim 13, with the exception of the following additional steps.

The statistical information is cryptographically signed within the postal security device. This yields a signature. (See paragraph 11)

The information and signature are communicated to the memory within the host. It should be appreciated that the information and signature are not communicated to the memory within the

postal security device. (See paragraphs 32 and 35)

The information and signature are communicated from the memory within the host to the cryptographic device. It should be appreciated that the information is not communicated from memory within the postal security device to the cryptographic device. (See paragraph 32)

(vi) Grounds of Rejection to be reviewed on Appeal

A. Whether the rejection of claim 1 (and claims 2-10) as supposedly rendered obvious by a two-way combination of US Patent No. 5,682,429 ("Cordery") and US Patent No. 6,868,443 ("Deslandes") is justified.

B. Whether the rejection of claim 11 (and claim 12) as supposedly rendered obvious by a two-way combination of US Patent No. 5,682,429 ("Cordery") and US Patent No. 6,868,443 ("Deslandes") is justified.

C. Whether the rejection of claim 13 (and claims 14-22) as supposedly rendered obvious by a two-way combination of US Patent No. 5,682,429 ("Cordery") and US Patent No. 6,868,443 ("Deslandes") is justified.

D. Whether the rejection of claim 23 (and claim 24) as supposedly rendered obvious by a two-way combination of US Patent No. 5,682,429 ("Cordery") and US Patent No. 6,868,443 ("Deslandes") is justified.

(vii) Argument

A. Whether the rejection of claim 1 (and claims 2-10) as supposedly rendered obvious by a

two-way combination of US Patent No. 5,682,429 ("Cordery") and US Patent No. 6,868,443 ("Deslandes") is justified.

Claim 1

Claim 1 is:

> A method for use with a postage meter system under the jurisdiction of a postal authority, the postage meter system comprising a host and a server, the host comprising a postal security device and postal indicia printing means, the server comprising a cryptographic device disposed for cryptographically secure communication with the postal security device, the method comprising the steps of:
>
> entering information into the host indicative of a batch of mail pieces to be franked;
>
> franking the mail pieces whilst storing information about the franking of the batch of mail pieces to a memory within the host;
>
> within the postal security device, performing a cryptographic authenticating procedure upon the information about the franking of the batch and the information indicative of the batch, said information defining statistical information;
>
> communicating the statistical information from the postal security device to the cryptographic device;
>
> authenticating the statistical information at the cryptographic device; and
>
> passing the statistical information to a postal authority.

In claim 1, the franking takes place *prior to* communication from the postal security device (which is within a host which also comprises a postal indicia printing means) to the cryptographic device (which is at a server). So far as the undersigned can discern, Cordery teaches away from this, teaching instead that various communications to and from some server occur *prior to* any franking by a postage meter.

The sequence of the steps cannot be ignored in considering this or any claim.

It is also noted that in the claim, it is the communication from the postal security device (which is within a host which also comprises a postal indicia printing means) *to the* cryptographic device (which is at a server), that is cryptographically authenticated. In contrast, so far as the undersigned can discern, in Cordery the only use of encryption is in connection with certain communications from the post office back to the mailer.

By teaching that the cryptographic communications be in the opposite direction from that set forth in the claim, Cordery appears to teach away in a second distinct way from the invention.

Finally, it will be appreciated that not all uses of cryptography are identical to each other. One use of cryptography, perhaps the use most familiar to lay persons, is encryption, which makes it difficult or impossible for an eavesdropper to learn the content of a message. A very different use of cryptography is authentication, which permits the receiver of a message to know that the sender is who it claims to be. This latter use is typically accomplished by cryptographic signing of a message or of a message digest or hash. These uses (encryption and authentication) are not at all the same thing.

Cordery, as best understood by the undersigned, speaks only of encryption uses. The claim, in contrast, speaks of authentication. As such, it appears that Cordery teaches away from the invention in this third distinct way.

For all these reasons it is requested that the rejection of claim 1 be reconsidered. Claims 2 through 12 should be allowed for the same reasons as claim 1.

Several additional arguments are provided below specifically for Claims 2-4, 6-8, and 11-12.

Claim 2

Claim 2 is:

> The method of claim 1 wherein
>
> the step of performing the cryptographic authenticating procedure comprises calculating a message authentication code, and
>
> the step of authenticating the statistical information comprises checking for correctness of the message authentication code.

The undersigned has diligently studied the cited portion of Cordery (col. 2, line 25-65) and is unable to find message authentication codes anywhere in the cited portion. The rejection should be reversed.

Claim 3

Claim 3 is:

> The method of claim 1 wherein
>
> the step of performing the cryptographic authenticating procedure comprises digitally signing the statistical information, and
>
> the step of authenticating the statistical information comprises checking for correctness of the digital signature.

The undersigned has diligently studied Cordery and is unable to find digital signing anywhere mentioned. The Examiner has not disclosed where this limitation can be found in Cordery nor Delandes. The rejection should be reversed.

Claim 4

Claim 4 is:

> The method of claim 1 wherein the communicating step further comprises establishing a cryptographically secure session and communicating the information in a cryptographically secure fashion.

The undersigned has diligently studied Cordery and is unable to find this limitation anywhere mentioned. The Examiner has not disclosed exactly where this limitation can be found in Cordery nor Delandes. The rejection should be reversed.

Claim 6

Claim 6 is:

> The method of claim 1 further comprising
>
> the step of passing a confirmation from the cryptographic device to the postal security device indicative of receipt by the cryptographic device from the postal security device, and
>
> the further step of deleting the statistical information from the postal security device upon receipt of the confirmation.

The Examiner has not disclosed exactly where this limitation can be found in Cordery nor Delandes. The rejection should be reversed.

Claim 7

Claim 7 is:

> The method of claim 1 further comprising the step, performed by the postal authority, of granting a discount based on the statistical information.

The Examiner bases the rejection on column 2, lines 25 of Cordery. Nowhere in Cordery is the undersigned able to find anything remotely resembling this limitation. The rejection should be

reversed.

Claim 8

Claim 8 is:

> The method of claim 1 further comprising the step, performed by the postal authority, of granting a credit for future franking based on the statistical information.

The Examiner bases the rejection on column 2, lines 25 of Cordery. Nowhere in Cordery is the undersigned able to find anything remotely resembling this limitation. The rejection should be reversed.

B. Whether the rejection of claim 11 (and claim 12) as supposedly rendered obvious by a two-way combination of US Patent No. 5,682,429 ("Cordery") and US Patent No. 6,868,443 ("Deslandes") is justified.

Claim 11

Claim 11 is:

> The method of claim 1 where the step of communicating the statistical information from the postal security device to the cryptographic device further comprises the steps of:
>
> cryptographically signing the statistical information within the postal security device, yielding a signature;
>
> communicating the information and signature to memory within the host and not within the postal security device;
>
> storing the information and signature within the memory within the host and not within the postal security device, and
>
> communicating the information and signature from memory within the host and

not within the postal security device, to the cryptographic device.

The Examiner bases the rejection on column 2, lines 25 of Cordery. Nowhere in Cordery is the undersigned able to find anything remotely resembling this limitation. The Examiner was requested in response to the June 14, 2005 Office Action to point out by page and line where these four limitations could be found, or to withdraw the rejection of claim 11. The Examiner has not provided page and line where the limitations can be found. The rejection should be reversed.

An additional argument for claim 12 is provided below.

Claim 12

Claim 12 is:

> The method of claim 11 wherein the storing of the information and signature within the memory within the host and not within the postal security device is for at least one day.

The Examiner bases the rejection on column 2, lines 25 of Cordery. Nowhere in Cordery is the undersigned able to find anything remotely resembling this limitation. The rejection should be reversed.

C. Whether the rejection of claim 13 (and claims 14-22) as supposedly rendered obvious by a two-way combination of US Patent No. 5,682,429 ("Cordery") and US Patent No. 6,868,443 ("Deslandes") is justified.

Claim 13 is:

A method for use with a postage meter system under the jurisdiction of a postal

authority, the postage meter system comprising a host and a server, the host comprising a postal security device and postal indicia printing means, the server comprising a cryptographic device disposed for cryptographically secure communication with the postal security device, the host operated by a service provider providing service to a plurality of users, the method comprising the steps of:

entering information into the host indicative of a batch of mail pieces to be franked and indicative of an identity of a user associated with the batch;

franking the mail pieces whilst storing information about the franking of the batch of mail pieces to a memory within the host;

within the postal security device, performing a cryptographic authenticating procedure upon the information about the franking of the batch and the information indicative of the batch, said information defining statistical information;

communicating the statistical information from the postal security device to the cryptographic device;

authenticating the statistical information at the cryptographic device; and

passing the statistical information to a postal authority.

In claim 13, the franking takes place *prior to* communication from the postal security device (which is within a host which also comprises a postal indicia printing means) to the cryptographic device (which is at a server). So far as the undersigned can discern, Cordery teaches away from this, teaching instead that various communications to and from some server occur *prior to* any franking by a postage meter.

The sequence of the steps cannot be ignored in considering this or any claim.

It is also noted that in the claim, it is the communication from the postal security device (which is within a host which also comprises a postal indicia printing means) *to the* cryptographic device (which is at a server), that is cryptographically authenticated. In contrast, so far as the

undersigned can discern, in Cordery the only use of encryption is in connection with certain communications from the post office back to the mailer.

By teaching that the cryptographic communications be in the opposite direction from that set forth in the claim, Cordery appears to teach away in a second distinct way from the invention.

Finally, it will be appreciated that not all uses of cryptography are identical to each other. One use of cryptography, perhaps the use most familiar to lay persons, is encryption, which makes it difficult or impossible for an eavesdropper to learn the content of a message. A very different use of cryptography is authentication, which permits the receiver of a message to know that the sender is who it claims to be. This latter use is typically accomplished by cryptographic signing of a message or of a message digest or hash. These uses (encryption and authentication) are not at all the same thing.

Cordery, as best understood by the undersigned, speaks only of encryption uses. The claim, in contrast, speaks of authentication. As such, it appears that Cordery teaches away from the invention in this third distinct way.

For all these reasons it is requested that the rejection of claim 13 be reconsidered. Claims 12 through 24 should be allowed for the same reasons as claim 13.

Several additional arguments are provided below specifically for Claims 14-16 and 18-20.

Claim 14

Claim 14 is:

> The method of claim 13 wherein
>
> the step of performing the cryptographic authenticating procedure comprises

calculating a message authentication code, and

the step of authenticating the statistical information comprises checking for correctness of the message authentication code.

The undersigned has diligently studied the cited portion of Cordery (col. 2, lines 25-65) and is unable to find message authentication codes anywhere in the cited portion. The rejection of Claim 14 should be reversed.

Claim 15

Claim 15 is:

The method of claim 13 wherein

the step of performing the cryptographic authenticating procedure comprises digitally signing the statistical information, and

the step of authenticating the statistical information comprises checking for correctness of the digital signature.

The undersigned has diligently studied Cordery and is unable to find digital signing anywhere mentioned. In the response to the June 14, 2005 Office Action, the Examiner was requested to point out exactly where this limitation could be found, or otherwise to withdraw the rejection of Claim 15. This request was not met. The rejection of Claim 15 should be reversed.

Claim 16

Claim 16 is:

The method of claim 13 wherein the communicating step further comprises establishing a cryptographically secure session and communicating the information in a cryptographically secure fashion.

The undersigned has diligently studied Cordery and is unable to find this limitation mentioned anywhere. In the response to the June 14, 2005 Office Action, the Examiner was requested to point out exactly where this limitation could be found, or otherwise to withdraw the rejection of Claim 16. This request was not met. The rejection of Claim 16 should be reversed.

Claim 18

Claim 18 is:

> The method of claim 13 further comprising
>
> the step of passing a confirmation from the cryptographic device to the postal security device indicative of receipt by the cryptographic device from the postal security device, and
>
> the further step of deleting the statistical information from the postal security device upon receipt of the confirmation.

Nowhere in Cordery is the undersigned able to find either of these steps. The rejection should be reversed.

Claim 19

Claim 19 is:

> The method of claim 13 further comprising the step, performed by the postal authority, of granting a discount to the user associated with the batch based on the statistical information.

Nowhere in Cordery is the undersigned able to find anything remotely resembling this limitation. The rejection of Claim 19 should be reversed.

Claim 20

Claim 20 is:

> The method of claim 13 further comprising the step, performed by the postal authority, of granting a credit for future franking to the user associated with the batch based on the statistical information.

Nowhere in Cordery is the undersigned able to find anything remotely resembling this limitation.

The rejection of Claim 20 should be reversed.

D. Whether the rejection of claim 23 (and claim 24) as supposedly rendered obvious by a two-way combination of US Patent No. 5,682,429 ("Cordery") and US Patent No. 6,868,443 ("Deslandes") is justified.

Claim 23

Claim 23 is:

> The method of claim 13 where the step of communicating the statistical information from the postal security device to the cryptographic device further comprises the steps of:
>
> cryptographically signing the statistical information within the postal security device, yielding a signature;
>
> communicating the information and signature to memory within the host and not within the postal security device;
>
> storing the information and signature within the memory within the host and not within the postal security device, and

communicating the information and signature from memory within the host and not within the postal security device, to the cryptographic device.

Nowhere in Cordery is the undersigned able to find anything remotely resembling these four limitations. The Examiner was requested in the response to the June 14, 2005 Office Action to point out by page and line where these four limitations could be found, or to withdraw the rejection of claim 23. This request was not met. The rejection should be reversed.

Claim 24

Claim 24 is:

> The method of claim 23 wherein the storing of the information and signature within the memory within the host and not within the postal security device is for at least one day.

Nowhere in either of the cited references is the undersigned able to find anything remotely resembling this limitation. The rejection of Claim 24 should be reversed.

Respectfully submitted,

/s/

Carl Oppedahl

PTO Reg. No. 32,746
Oppedahl & Olson, LLP
PO Box 5388
Dillon, CO 80435-5068
telephone 970-468-8600

Claims Appendix

1. A method for use with a postage meter system under the jurisdiction of a postal authority, the postage meter system comprising a host and a server, the host comprising a postal security device and postal indicia printing means, the server comprising a cryptographic device disposed for cryptographically secure communication with the postal security device, the method comprising the steps of:

entering information into the host indicative of a batch of mail pieces to be franked;

franking the mail pieces whilst storing information about the franking of the batch of mail pieces to a memory within the host;

within the postal security device, performing a cryptographic authenticating procedure upon the information about the franking of the batch and the information indicative of the batch, said information defining statistical information;

communicating the statistical information from the postal security device to the cryptographic device;

authenticating the statistical information at the cryptographic device; and

passing the statistical information to a postal authority.

2. The method of claim 1 wherein the step of performing the cryptographic authenticating procedure comprises calculating a message authentication code, and the step of authenticating the statistical information comprises checking for correctness of the message authentication code.

3. The method of claim 1 wherein the step of performing the cryptographic authenticating procedure comprises digitally signing the statistical information, and the step of authenticating the statistical information comprises checking for correctness of the digital signature.

4. The method of claim 1 wherein the communicating step further comprises establishing a cryptographically secure session and communicating the information in a cryptographically secure fashion.

5. The method of claim 1 wherein the communicating step is performed in the absence of the establishment of a cryptographically secure session.

6. The method of claim 1 further comprising the step of passing a confirmation from the cryptographic device to the postal security device indicative of receipt by the cryptographic device from the postal security device, and

the further step of deleting the statistical information from the postal security device upon receipt of the confirmation.

7. The method of claim 1 further comprising the step, performed by the postal authority, of granting a discount based on the statistical information.

8. The method of claim 1 further comprising the step, performed by the postal authority, of granting a credit for future franking based on the statistical information.

9. The method of claim 1 wherein the memory within the host is within the postal security device.

10. The method of claim 1 wherein the memory within the host is not within the postal security device.

11. The method of claim 1 where the step of communicating the statistical information from the postal security device to the cryptographic device further comprises the steps of:

cryptographically signing the statistical information within the postal security device, yielding a signature;

communicating the information and signature to memory within the host and not within the postal security device;

the information and signature within the memory within the host and not within the postal security device, and

communicating the information and signature from memory within the host and not within the postal security device, to the cryptographic device.

12. The method of claim 11 wherein the storing of the information and signature within the memory within the host and not within the postal security device is for at least one day.

13. A method for use with a postage meter system under the jurisdiction of a postal authority, the postage meter system comprising a host and a server, the host comprising a postal security device and postal indicia printing means, the server comprising a cryptographic device disposed for cryptographically secure communication with the postal security device, the host operated by a service provider providing service to a plurality of users, the method comprising the steps of:

entering information into the host indicative of a batch of mail pieces to be franked and indicative of an identity of a user associated with the batch;

franking the mail pieces whilst storing information about the franking of the batch of mail pieces to a memory within the host;

within the postal security device, performing a cryptographic authenticating procedure upon the information about the franking of the batch and the information indicative of the batch, said information defining statistical information;

communicating the statistical information from the postal security device to the cryptographic device;

authenticating the statistical information at the cryptographic device; and

passing the statistical information to a postal authority.

14. The method of claim 13 wherein the step of performing the cryptographic authenticating procedure comprises calculating a message authentication code, and the step of authenticating the statistical information comprises checking for correctness of the message authentication code.

15. The method of claim 13 wherein the step of performing the cryptographic authenticating procedure comprises digitally signing the statistical information, and the step of authenticating the statistical information comprises checking for correctness of the digital signature.

16. The method of claim 13 wherein the communicating step further comprises establishing a cryptographically secure session and communicating the information in a cryptographically secure fashion.

17. The method of claim 13 wherein the communicating step is performed in the absence of the establishment of a cryptographically secure session.

18. The method of claim 13 further comprising the step of passing a confirmation from the cryptographic device to the postal security device indicative of receipt by the cryptographic device from the postal security device, and the further step of deleting the statistical information from the postal security device upon receipt of the confirmation.

19. The method of claim 13 further comprising the step, performed by the postal authority, of granting a discount to the user associated with the batch based on the statistical information.

20. The method of claim 13 further comprising the step, performed by the postal authority, of granting a credit for future franking to the user associated with the batch based on the statistical information.

21. The method of claim 13 wherein the memory within the host is within the postal security device.

22. The method of claim 13 wherein the memory within the host is not within the postal security device.

23. The method of claim 13 where the step of communicating the statistical information from the postal security device to the cryptographic device further comprises the steps of:

cryptographically signing the statistical information within the postal security device, yielding a signature;

communicating the information and signature to memory within the host and not within the postal security device;

storing the information and signature within the memory within the host and not within the postal security device, and

communicating the information and signature from memory within the host and not within the postal security device, to the cryptographic device.

24. The method of claim 23 wherein the storing of the information and signature within the memory within the host and not within the postal security device is for at least one day.

Evidence Appendix

The following references cited by the Examiner in the December 02, 2005 Office Action are included within this Appendix.

1. A copy of US Patent No. 5,682,429

2. A copy of US Patent No. 6,868,443

Related Proceedings Appendix

NONE